Department of Homeland Security Daily Open Source Infrastructure Report for 27 June 2006

Current Nationwide Threat Level is ELEVATED — Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The Nuclear Regulatory Commission has issued its first license in 30 years for a major commercial nuclear facility, allowing an international consortium to build the nation's first private fuel source for commercial nuclear power plants. (See item 3)
- The Associated Press reports continuing heavy rains are causing flooding across the mid−Atlantic region, washing out roads, disrupting Amtrak's Northeast Corridor service, and forcing evacuations. (See item 12)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *June 26, Dow Jones* — **Exxon Baytown upset cause two acid gas releases.** A pollution control unit at Exxon Mobil Corp.'s giant Baytown, TX, refinery suffered two upsets Saturday, June 25, that caused two emissions of acid gas about 12 hours apart, according to reports. The Girbotol unit, used to remove hydrogen sulfide from refinery gases, malfunctioned Saturday morning, resulting in the emission of sulfur dioxide, carbon monoxide, nitrogen oxides, as well as hydrogen sulfide, said one report to the Texas Commission on Environmental Quality. The unit was returned to normal operations after each incident. The cause of the malfunction is under investigation. The emissions events brought the week's total for the plant to four. On June

16, a 90,000 barrel−a−day fluid catalytic cracker (FCC) tripped, and then tripped again on June 20.
Source: http://news.morningstar.com/news/DJ/M06/D26/200606260725DOWJONESDJONLINE000210.html?Cat=Energy

2. *June 25, Associated Press* — **Man charged with using device to steal gasoline.** An Albuquerque, NM man has been accused of manipulating a gasoline pump and filling up several cans with unleaded fuel and a large tank with hundreds of gallons of diesel. The man was arrested Friday, June 23, after State Police Officer Augustine Samaniego spotted him filling up at a Conoco station. The owner of the station had recently called police about missing fuel. The fuel pump's electronic display showed an unusual message and registered about 800 gallons of diesel at over $2,000. Morales told the officer that his boss met him at the pumps with a credit card, initiated the transaction, and drove away. In addition to the large tank, Morales had seven gas cans in the back of his truck. Police believe some type of card or device was used to override the pump. The device wasn't recovered, so police are warning stations to monitor their fuel sales.
Source: http://www.freenewmexican.com/news/45518.html

3. *June 25, Associated Press* — **U.S. grants first license for major nuclear plant in 30 years.** The Nuclear Regulatory Commission has issued its first license for a major commercial nuclear facility in 30 years, allowing an international consortium to build what will be the nation's first private fuel source for commercial nuclear power plants. Construction of the $1.5 billion National Enrichment Facility could begin in August, and the plant could be ready to sell enriched uranium by early 2009, said James Ferland, president of the consortium of nuclear companies, Louisiana Energy Services. The plant, licensed on Friday, June 23, will be built near the small southeastern New Mexico community of Eunice. A Kentucky facility owned by the Department of Energy and operated by a former federal corporation that has been privatized is currently the only source of enriched uranium for commercial U.S. nuclear power plants.
NEF Press Release: http://www.nefnm.com/documents/public/License_Release_6−23−0 6.pdf
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/06/24/AR2006062400838.html?nav=rss_nation

4. *June 25, Associated Press* — **Researchers look underwater for energy.** The Electric Power Research Institute has released a study concluding that underwater turbines powered by the tidal movement at three sites can produce electricity at a cost that competes with wind power and natural gas−powered power plants. According to the study, tidal power could produce electricity for 4.2 to 6.5 cents per kilowatt−hour at those three locations. The standard offer for Central Maine Power customers is 8.4 cents per kilowatt hour. Roger Bedard, project leader, provided a detailed analysis of the technological and economic feasibility of tidal resources at one site apiece in Maine, Massachusetts, California, Washington, and Alaska, and in two Canadian provinces, New Brunswick and Nova Scotia. The other two sites with the greatest potential were at San Francisco's Golden Gate Bridge, and in the Bay of Fundy at Minas Pass, Nova Scotia. So far, the Federal Energy Regulatory Commission has received 21 preliminary permit applications for tidal power projects, said spokesperson Celeste Miller. Ten have been granted and the others are pending, Miller said.
Source: http://www.boston.com/news/local/massachusetts/articles/2006/06/25/researchers_look_underwater_for_energy/

5. *June 25, Medill News Service* — **Report: Local nukes safe.** Three Mile Island Unit 1 and Peach Bottom Atomic Power Station, both located in Pennsylvania, are among the safest nuclear energy sites in the nation, according to a preliminary report released by the Government Accountability Office (GAO). The report says inspectors found 12 major violations at six plants −− none of which were at TMI or Peach Bottom −− in the past five years. Inspection letters for both plants, released twice a year, reported no more than five minor citations at either complex during any period since 2000. Most were because of human errors, such as TMI's failure to train workers in emergency responses and a Peach Bottom employee who falsified fire watch logs. The House Energy and Commerce Committee requested GAO to investigate whether the NRC needs to improve its safety monitoring system for 103 nuclear sites across the U.S. The GAO report states that since 2001, NRC inspectors found more than 4,000 violations among the nation's nuclear sites. But 97 percent of those were of low−safety significance, including all of the citations at TMI and Peach Bottom.
   Source: http://www.ydr.com/newsfull/ci_3978728

[Return to top]

Chemical Industry and Hazardous Materials Sector

6. *June 26, Cox Communications (CA)* — **Solvent−soaked rags cause fire in law offices.** Solvent−soaked rags are being blamed for sparking a fire in law offices downtown San Diego, CA, that caused over one−million−dollars in damage. Officials say the fire was reported Sunday morning, June 25, at the Bayview Corporate Center. A fire spokesperson said when temperatures drop and humidity rises, a chemical reaction occurs that causes solvent−soaked or oil−soaked rags to heat up and ignite.
   Source: http://sandiego.cox.net/cci/newslocal/local?_mode=view&view=LocalNewsArticleView&articleId=1576761

[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

7. *June 26, Australian IT* — **Error exposes bank files.** The details of 3,500 Australian customers from 18 banks, including names and account numbers, were lost when a classified computer dossier on Russian mafia "phishing" scams was misplaced by the Australian High Tech Crime Centre (AHTCC) in April last year. An AHTCC police officer lost a memory stick containing the dossier, between Sydney and London. The loss could reveal details of police inquiries into the organized crime networks operating in three countries, including Latvia and Estonia. The bungle comes at a time when eastern European crime gangs, including the Russian mafia, have become a growing threat in Australia with increasingly sophisticated phishing scams. The bank

customers, who had already fallen victim to the crime gangs by providing banking details to bogus e−mail requests, were never told their information had been exposed. AHTCC director Kevin Zuccato said the AHTCC was confident that even if the memory stick fell into the wrong hands, there was not enough personal information to enable any further fraud.
Source: http://australianit.news.com.au/articles/0,7204,19588463%5E15306%5E%5Enbv%5E,00.html

8. *June 24, Websense Security Labs* — **Phishing Alert: BellSouth.** Websense Security Labs has received reports of a new phishing attack that targets customers of BellSouth. Users receive a spoofed e−mail message, which claims that their account details must be updated to keep the account active. The message provides a link to a phishing Website that requests personal and financial information.
Source: http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =535

9. *June 24, Websense Security Labs* — **Phishing Alert: Ulster Bank.** Websense Security Labs has received reports of a new phishing attack that targets customers of Ulster Bank. Users receive a spoofed e−mail message, which claims that their account details must be verified due to software maintenance and system upgrades. The message provides a link to a phishing Website that requests users to log on and provide account details.
Source: http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =536

[Return to top]

Transportation and Border Security Sector

10. *June 26, Inside Bay Area (CA)* — **Airport security uses new method.** Behind the check−in counter for Southwest Airlines' Terminal 2 at California's Oakland International Airport there is a $16.4 million quartet of new machines, fully integrated into the terminal's baggage−handling conveyor system. After check in, the luggage is whisked around a conveyor system and shunted into one of four, minivan−sized CTX 9000 scanners, which get the first look at what is inside. Computer software in the machines matches what it sees to a database of suspicious shapes, densities, and combinations of objects. If a scan shows an apparent red−flag item, that bag is rolled along the conveyor to a nearby room, where inspectors from the Transportation Security Administration give it a closer look. The system processes 1,000 pieces of luggage an hour, as opposed to the 250 bags previously checked by hand, chemical swabs, bomb−sniffing dogs and stand−alone CTX scanners, said airport spokesperson Rosemary Barnes.
Source: http://www.insidebayarea.com/argus/localnews/ci_3981235

11. *June 26, ContraCostaTimes (CA)* — **Officials eye ferries to help ease congestion.** As Bay Area Rapid Transit, or BART, trains fill with passengers and Bay Area bridges clog with motorists, transportation officials hope to spur a renaissance in an often−overlooked form of commuting: ferries. "We see an opportunity not only to improve transportation in the Bay Area but to use ferry terminals as a catalyst for development," said Steve Castleberry, executive director of the Water Transit Agency. There are six ferry terminals scattered across the Bay, including ones in Larkspur, Vallejo, and San Francisco. Over the next 25 years, the Water Transit Agency, a new commission formed to enliven ferry service, hopes to create eight new

terminals throughout the region. Currently, 10,000 people a day ride ferries, Castleberry said. The Bay Area is the third−busiest ferry operator behind New York and Seattle. By 2025, ridership is expected to reach 30,000 a day.
Source: http://www.contracostatimes.com/mld/cctimes/news/transportat ion/14903925.htm

12. *June 26, Associated Press* — **Northeast flooding washes out roads, delays trains.** Heavy rains caused flooding across the mid−Atlantic region, washing out roads, disrupting Amtrak service, and forcing some evacuations. Amtrak's Northeast Corridor service between Philadelphia and Washington, DC, was disrupted early Monday, June 26, due to high water and washout conditions along tracks, caused by the weekend's heavy rainfall. The Washington Capital Beltway was closed by a mudslide near Alexandria, VA, that left debris piled up to five feet high on the roadway. Commuter rail lines into Washington had to cancel service because of high water from heavy rains Sunday night. Virginia Railway Express and Maryland's MARC train lines canceled service running into the nation's capital. Metro subway service in the city was also disrupted downtown for high water on the electrified rails, said Metro spokesperson Lisa Farbstein. On Maryland's Eastern Shore, Federalsburg Mayor Betty Ballas declared an emergency for the town of about 2,600 people Sunday, June 25. Donald Nagel, Federalsburg chief of police, said low−lying areas in the town were flooded Sunday morning, and about 45 people were voluntarily evacuated.
Source: http://www.cnn.com/2006/WEATHER/06/26/east.flood.ap/index.ht ml

13. *June 26, Examiner* — **Railroad officials slow trains to guard against derailment in heat.** Railroad officials issued a third heat order in as many days Friday, June 23, for MARC commuter trains traveling the Brunswick and Camden lines that connect Baltimore and Martinsburg, WV, with Washington, DC. The orders, issued by CSX, slow Maryland Transit Administration (MTA) trains and others traveling CSX rails so crews can check for warped rails that can lead to derailments, said MTA spokesperson Mabilia Reyes. CSX spokesperson Bob Sullivan said heat orders are triggered by days when temperatures fluctuate more than 40 degrees or when there have been several consecutive days where temperatures have reached 85 to 95 degrees. Sullivan said the railroad sends additional crews to check the rails from 1 to 7 p.m. on heat order days.
Source: http://www.examiner.com/a−160079~Railroad_officials_slow_tra ins_to_guard_against_derailment_in_heat.html

[Return to top]

Postal and Shipping Sector

14. *June 26, Memphis Business Journal (TN)* — **FedEx to expand in France.** FedEx Express and the French Office of Economic and Commercial Affairs (FOECA) will work together to expand France−U.S. trade, FedEx Corp. announced Monday, June 26. FedEx and FOECA will provide resources to small− and medium−sized French and U.S. businesses that want to import and export, Memphis−based FedEx Corp. said in the announcement. The FedEx−FOECA alliance will assist these businesses in finding international buyers and enter new markets. FedEx will generate awareness among its customers about the benefits of the FOECA export assistance network available in Atlanta, Chicago, Houston, New York, San Francisco and Washington, DC. The world's largest package shipper, FedEx employs about 30,000 in Memphis and

260,000 globally.
Source: http://memphis.bizjournals.com/memphis/stories/2006/06/26/da ily1.html

[Return to top]

Agriculture Sector

15. *June 26, Journal−Gazette (Indiana)* — **Hog rules set to change.** Farmers may have to adjust the way they administer medicine to hogs to comply with new Japanese food import standards. The rules will not allow hogs to be slaughtered immediately after certain antibiotics have been administered, which should prevent traces of the drugs from being present in their meat. The pork industry is being cautious. Japan, which banned U.S. beef for more than two years from worries about "mad cow" disease, is a key export market for U.S. pork. Japan buys about 750 million pounds of U.S. pork muscle a year, 45 percent of all U.S. pork exports at a value of more than one billion dollars, according to the U.S. Meat Export Federation. The National Pork Board says one animal in violation of Japanese product specifications could imperil that lucrative market. The rules limit the amount of residue from 799 feed additives, veterinary drugs and agricultural chemicals allowed in all food products, including pork. Old Japanese standards limited only 283 substances. Hog farmers use about 50 of the products on the new list, said Brian Richert, swine extension specialist at Purdue University in West Lafayette. The Japanese rules will affect the use of 15 or 16 of those products.
Source: http://www.fortwayne.com/mld/journalgazette/business/1490450 5.htm

16. *June 26, USAgNet* — **Insect threatens wine industry in Arizona.** Arizona agriculture officials are battling what they say could become an infestation of the glassy−winged sharpshooter, a leafhopper that carries bacterium deadly to grapevines. The bug found its way to southeast Arizona from California on a plant bound for a Sierra Vista nursery. So far this year, the state Agriculture Department has trapped 19 adults and found numerous egg masses in a three−mile range near Sierra Vista. Discovery of the sharpshooters in Sierra Vista is critical because the city sits between two major grape−growing areas: Sonoita and Elgin to the west, and the Sulphur Springs Valley to the east.
Glassy−winged sharpshooter information: http://www.cnr.berkeley.edu/xylella/oss.html
Source: http://www.usagnet.com/story−national.cfm?Id=1219&yr=2006

[Return to top]

Food Sector

Nothing to report.
[Return to top]

Water Sector

17. *June 26, Los Angeles Times* — **E. coli found in Gorman, California water.** The bacteria E. coli has been detected in the water distribution system that serves Gorman, CA, health officials said Sunday, June 25. Restaurants have been forced to close and residents have been warned to

boil their water to avoid getting sick. In documents posted around town, the Golden Valley Municipal Water District said the bacteria, which can cause severe gastrointestinal problems, was first detected Thursday, June 22. The documents say the water agency is collecting water samples to determine the source of the problem, and is flushing out the distribution system. Richard Wagener, director of environment protection for the Los Angeles County Department of Health Services' Division of Environmental Health, said health officials took new water samples Saturday, June 24. Those samples were clean, and once a second consecutive sample is clear of contamination, the boiled−water order will be lifted.
Source: http://www.latimes.com/news/printedition/california/la−me−water26jun26,1,118784.story?coll=la−headlines−pe−california&ct rack=1&cset=true

18. *June 22, Mountain View Telegraph (NM)* — **Moriarty, New Mexico confounded by water surge.** An unexpected surge of water into Moriarty, NM's wastewater treatment plant has city staff and even the mayor searching for clues. The mysterious water surge first appeared on May 28, Mayor Adan Encinias said during a June 13 meeting of the Moriarty City Council. City staff noticed that the plant was receiving 120,000 gallons more sewage than usual that day, even though city wells were not pumping more fresh water than normal. Then on June 4, about 100,000 gallons of water appeared in the city's sewer system. It happened again on June 13. During the evening of June 13, the wastewater plant took in more than 300,000 gallons of water −− more than the entire city uses during an average full day in the summer. On June 4 and 13, city wells did not pump more water than usual.
Source: http://www.mvtelegraph.com/mountain/470572mtnview06−22−06.ht m

[Return to top]

Public Health Sector

19. *June 27, Sydney Morning Herald (Australia)* — **Flu deaths traced to swans.** Four people have died after catching avian flu from swans in the first confirmed cases of the disease being passed from wild birds, scientists have revealed. The victims, from a village in Azerbaijan, are believed to have caught the H5N1 virus earlier this year when they plucked the feathers from dead birds to sell for pillows. Three other people were infected but survived. Andreas Gilsdorf, an epidemiologist at the Robert Koch Institute in Berlin, who led the team that made the discovery, said: "As far as we know this is the first transmission from a wild bird, but it was a very intensive contact." Almost all of the 220 other confirmed human cases of bird flu, including 130 deaths, have been linked to domestic poultry. The cases in the Salyan district of southeast Azerbaijan were first reported in March. Six of the seven, aged between 10 and 20, were from the same family.
Source: http://www.smh.com.au/news/world/flu−deaths−traced−to−swans/2006/06/26/1151174135524.html

20. *June 23, Agence France−Presse* — **West African ministers meet on strategies to fight bird flu.** West African ministers adopted a plan for fighting the outbreak of avian influenza in the region and preventing its spread to humans. The plan, which includes setting up an emergency fund, was agreed at the end of a one−day meeting in the Nigerian capital, organized by the Economic Community of West African States (ECOWAS) of ministers in charge of agriculture, health, livestock, environment and integration. The meeting was attended by 13 of the 15

ECOWAS countries −− Liberia and Cape Verde were absent −−− and two non−ECOWAS countries, Mauritania and Chad. Representatives of other international organizations, farmer organizations, civil society groups and development partners also took part in the talks. Nigeria became the first African country where the disease was reported in January this year. Officials said the outbreak in Africa's most populous country poses a potential threat to human life and could cause severe economic losses in the poultry industry. It is also feared that the disease could spread to other neighboring West African countries if not contained. So far, there have been confirmed reports of the disease on poultry farms in more than a dozen Nigerian states, but no human case has yet been reported.
Source: http://news.yahoo.com/s/afp/20060623/hl_afp/healthfluwestafrica_060623220519;_ylt=Aibw1ioQZOg6cUIuVxmlNtOJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

21. *June 25, Arkansas Democrat Gazette* — **State uncertain if plan's enough.** The Arkansas Department of Emergency Management is not confident that the state's emergency plan is adequate to manage a major catastrophe, with the biggest gaps in the areas of evacuations and shelters. Parts of the plan simply haven't been put in writing −− like "a timeline of when people would do what in a disaster," said David Maxwell, the emergency agency's deputy director. Other aspects have never been fully developed, partly because the need wasn't uncovered until Hurricane Katrina exposed emergency planning failures and weaknesses at all levels of government. Emergency officials are fixing the plan −− and believe they can handle most emergencies −− but don't know when the more weighty issues will be resolved. The state bluntly detailed the flaws for the Department of Homeland Security in a self−assessment, which Maxwell said he did not know would be made public. According to the self−assessment, Arkansas gave its catastrophe plan the lowest possible marks in all nine categories −− far worse scores than federal reviewers gave the plan.
Source: http://www.nwarktimes.com/adg/News/158647/

22. *June 25, Journal Gazette (IN)* — **Safety academy nearing fruition in Indiana.** Six years ago, the Fort Wayne, IN, police and fire chiefs came to Mayor Graham Richard asking for new training academies. After contemplating how to sell the cost of those buildings to the City Council, Richard realized there was a solution that would not only save money but likely improve public safety and communications between the two agencies. He said he would support new academies for the police and fire, so long as they were located in one building. This spawned the idea for what will be the $27 million Regional Public Safety Academy, for which construction will begin Wednesday, July 5, at the site of the former Southtown Mall. The 132,000−square−foot academy will include 13 classrooms −− six set up for distance learning

−− locker rooms, a gymnasium, simulators, a 16−lane pistol range and 600 parking spaces. Richard said the academy will strengthen regional safety, increase interest in public safety career fields and improve communication between different safety organizations.
Source: http://www.fortwayne.com/mld/fortwayne/news/local/14897258.h tm

23. *June 24, Journal News (NY)* — **Rockland, New York, pushing for new emergency services system.** Rockland, NY, emergency workers might not be able to communicate if a major disaster such as a plane crash or hurricane were to hit tomorrow. Time is running out on eight radio frequencies that Rockland needs to allow emergency personnel to communicate at the same time. The frequencies will expire in September if the county doesn't show progress on its radio communications project. Rockland's communication gaps are caused by everything from the county's peaks and valleys to a variety of equipment and radio bandwidths. Currently, all the county's police departments can communicate with one another in an emergency. So can the 26 fire departments, except when the county's hilly topography creates dead zones. Additionally, the police can speak to the ambulance workers, but the fire departments can't.
Source: http://www.thejournalnews.com/apps/pbcs.dll/article?AID=/200 60624/NEWS03/606240315/1026/NEWS10

[Return to top]

Information Technology and Telecommunications Sector

24. *June 26, VNUNet* — **Computers set for 500−fold magnetic power boost.** Nanotech magnetic fields that replace traditional wiring in silicon chips could make computers up to 500 times more powerful, European scientists have claimed. The University of Bath is to lead an international $1,010,500 three−year project to develop a system which could cut out the need for wiring in processor chips. The project will look at ways of producing microwave energy on a small scale by firing electrons into magnetic fields produced in semi−conductors that are only a few atoms wide and are layered with magnets.
Source: http://www.vnunet.com/vnunet/news/2159091/computers−set−500− fold−magnetic

25. *June 26, VNUNet* — **Belgium to embrace Open Document Format.** The federal government of Belgium plans to switch to the Open Document Format (ODF) by September 2008. The move could bode ill for Microsoft, since the company's Office products do not support the format. Belgium is aiming to prevent a vendor lock−in, allowing the state to access data with any application that supports the open format. It is the first nation to openly embrace ODF. The State of Massachusetts revealed in September that it would start mandating government agencies to support the format by January 2007.
Source: http://www.vnunet.com/vnunet/news/2159039/belgium−embrace−op en−document

26. *June 26, Register (UK)* — **'Malicious damage' causes Telewest World Cup blackout.** Around 100,000 homes in the Bristol and Cotswolds areas of the UK were left without TV or Internet services Sunday, June 25, after two NTL:Telewest cables were "maliciously damaged." Access was restored to most customers Monday, June 26.
Source: http://www.theregister.co.uk/2006/06/26/telewest_cable/

27. *June 23, VNUNet* — **IBM gives away Java security software.** IBM plans to give away software to encourage developers to build security into their business applications, and better protect against hackers, identity thieves and malicious users. The software will allow Java developers to more easily engineer security into the software lifecycle process at the beginning of their design, rather than plugging security holes with patches after the damage is done. The free technologies are hosted on IBM alphaWorks, the firm's online outlet for emerging technologies. The code will provide increased security for Java applications, and automated encryption of information shared across networks.
Source: http://www.vnunet.com/vnunet/news/2158939/ibm−gives−away−jav a−security

28. *June 23, VNUNet* — **Gartner blasts claims of cyber−crime decline.** Businesses should pay no attention to a survey from the Computer Security Institute (CSI) claiming that cyber−crime damage is on the decline, analyst firm Gartner has warned. Its study carries weight because it is conducted with the Federal Bureau of Investigations. The results of the survey prompted the CSI to claim that the extent of today's security threats is "overstated," but Gartner warned that surveys often do not portray objective reality. In addition, the study lacks a consistent loss model that properly reflects changes in the online security space, according to Gartner.
Source: http://www.vnunet.com/vnunet/news/2158921/gartner−blasts−sec urity−surveys

29. *June 22, Secunia* — **IBM HMC sendmail and OpenSSH vulnerabilities.** IBM has acknowledged a vulnerability and a weakness in IBM HMC, which can be exploited by, local users to perform certain actions with escalated privileges, and to compromise a vulnerable system. Analysis: scp in OpenSSH 4.2p1 allows attackers to execute arbitrary commands via filenames that contain shell metacharacters or spaces. The vulnerability and weakness have been reported in version 5.2.1 (V5 R2.1). Solution: Apply security fix MH00688: http://www14.software.ibm.com/webapp/set2/sas/f/hmc/power5/d ownload/v521.Update.html
Source: http://secunia.com/advisories/20723/

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of active exploitation of a new vulnerability in Microsoft Excel. Successful exploitation could allow an attacker to execute arbitrary code with the privileges of the user running Excel. For more information please the review the following:

Technical Cyber Security Alert: TA06−167A
http://www.us−cert.gov/cas/techalerts/TA06−167A.html

Vulnerability Note: VU#802324 http://www.kb.cert.org/vuls/id/802324

We are continuing to investigate this vulnerability. US−CERT recommends the following actions to help mitigate the security risks:

Install anti−virus software, and keep its virus signature files up to date.

Limit user privileges to no administrator rights.

Save and scan any attachments before opening them.

Review the workarounds described in Microsoft Security Advisory 921365: http://www.microsoft.com/technet/security/advisory/921365.ms px

US−CERT strongly encourages users not to open unfamiliar or unexpected email attachments, even if sent by a known and trusted source. Users may wish to read Cyber Security Tip ST04−010 for more information on working with email attachments: http://www.us−cert.gov/cas/tips/ST04−010.html

FDIC Phishing Scam

US−CERT continues to receive reports of phishing scams that target online users. Recently, the phishing scam targeted the customers of Federal Deposit Insurance Company (FDIC) insured institutions.

Customers of FDIC institutions received a spoofed email message, which claims that their account is in violation of the Patriot Act, and that FDIC insurance has been removed from their account until their identity can be verified. The message provides a link to a malicious web site which prompts users to enter their customer account and identification information.

If you were affected by the FDIC phishing scam, please refer to the FDIC Consumer Alert for assistance: http://www.fdic.gov/consumers/consumer/alerts/phishing.html

US−CERT confirms that the federal agencies including Department of Homeland Security (DHS) mentioned in the fraudulent email have not sent out an email that requests customer account or identification information.

US−CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US−CERT: http://www.us−cert.gov/nav/report_phishing.html

Non−federal agencies and other users should report phishing incidents to OnGuard Online, a consortium of Federal Agencies: http://onguardonline.gov/phishing.html

Additionally, users are encouraged to take the following measures to prevent phishing attacks from occurring:

Do not follow unsolicited web links received in email messages.

Contact your financial institution and file a complaint with the Federal Trade Commission (FTC) immediately if you believe your account or financial information has been compromised.
https://rn.ftc.gov/pls/dod/widtpubl$.startup?Z_ORG_CODE=PU03

Review FTC's web site on how to protect yourself from identity theft:
http://www.consumer.gov/idtheft/

Review the OnGuard Online practical tips to guard against Internet fraud, secure your computer, and protect your personal information:
http://onguardonline.gov/phishing.html

Refer to the US−CERT Cyber Security Tip on Avoiding Social Engineering and Phishing Attacks: http://www.us−cert.gov/cas/tips/ST04−014.html

Refer to the CERT Coordination Center document on understanding Spoofed/Forged Email: http://www.cert.org/tech_tips/email_spoofing.html

PHISHING SCAMS

US−CERT continues to receive reports of phishing scams that target online users and Federal government web sites. US−CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US−CERT.
http://www.us−cert.gov/nav/report_phishing.html

Non−federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. http://onguardonline.gov/phishing.html

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 445 (microsoft−ds), 38566 (−−−), 25 (smtp), 24232 (−−−), 80 (www), 50497 (−−−), 135 (epmap), 4672 (eMule), 54856 (−−−) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

30.

June 26, Reuters (UK) — **Wimbledon security tight over bombs anniversary.** Wimbledon has tightened security at this year's tournament after last year's suicide bomb attacks in London, police said on Monday, June 26. But detectives stressed that they had no intelligence to suggest that the two−week championships was a specific target. Organizers said Wimbledon would mark the first anniversary of the attacks on the transport system in central London with a two−minute silence next Friday, July 7. This year all tennis fans buying day tickets to Wimbledon are being checked through airport−style scanners. Chief Superintendent Michael Wood said planning, preparation and contingency plans for tournament security had been reviewed after last year's attacks that killed 52 people.
Source: http://today.reuters.co.uk/news/newsArticle.aspx?type=tennisNews&storyID=2006−06−26T174913Z_01_L26581977_RTRIDST_0_SPORT−TENNIS−WIMBLEDON−SECURITY.XML

[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer